IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NORTH DAKOTA

UNITED STATES OF AMERICA, Plaintiff, v. NICHOLAS JAMES MORGAN-DEROSIER, Defendant.	Case No. 3:22-cr-05 **UNITED STATES' RESPONSE TO DEFENDANT'S MOTION TO SUPPRESS EVIDENCE**

The United States of America, by Mac Schneider, United States Attorney for the District of North Dakota, and Jennifer Klemetsrud Puhl, First Assistant United States Attorney, and Charles Schmitz, Trial Attorney, United States Department of Justice, hereby responds to Defendant Nicholas James Morgan-Derosier's (Defendant) Motion to Suppress Evidence (Doc. 69) seized from various media in his residence.

I. INTRODUCTION

Defendant raises several arguments that the warrant is both underinclusive and overbroad. Most of Defendant's arguments are *not* that the warrant and accompanying affidavit fail to contain probable cause, or various limiting principles (crimes, date restrictions, file-type restriction, etc.), but that the warrant and affidavit fail to list those items in the "right" places. The warrant does, however, contain a clerical error that the search was authorized for Defendant's "person" rather than his "person and his premises," but the Eighth Circuit Court of Appeals has already opined on basically the same clerical error and has found that good faith nevertheless applied. Defendant's arguments, which are without merit, are considered below in turn.

II. BACKGROUND

A. Financial Investigation

Defendant owned and operated Team Lawn, Inc., a landscaping and construction business. On October 15, 2019, the Grand Forks County District Court issued an Order of Injunction and [Order] To Comply, enjoining Defendant and his business from engaging in any sale of services, including services as a contractor. See Attachment 1. This same Order suspended Defendant's contractor license until further order of the Court.

Thereafter, Grand Forks Police Department (GFPD) Detective David Buzzo was assigned to investigate a fraudulent check involving Team Lawn, Inc. As part of that investigation, Detective Buzzo spoke with an investigator with the Attorney General's Consumer Protection and Anti-Trust Division. During their conversation, Detective Buzzo learned that Defendant was still doing business in North Dakota, thereby violating the above-mentioned Order and N.D.C.C. § 43-07-02 (License required--Construction Fraud—Penalty).

Specifically, the Attorney General's Investigator informed Detective Buzzo that he had received a complaint from Jack Hirst, a former employee of Team Lawn, Inc. The Investigator sent Detective Buzzo the materials that he had received from Hirst which reflected, among other things, that Defendant was still operating his landscaping and construction business, albeit under a different name. Detective Buzzo also determined that Defendant and his businesses—Team Lawn & Landscape and Derosier Outdoors—

were receiving mail at 412 5th Avenue South in Grand Forks, North Dakota. This is the same address where Defendant and several of his employees were then residing.

Detective Buzzo confirmed with the North Dakota Secretary of State that Dersoier Outdoors was not a registered business in North Dakota nor did it have a contractor's license. Detective Buzzo also conducted an open-source internet search and discovered job postings for Derosier Outdoors on Craigslist and JobTerro, dated July 27, 2020, and July 28, 2020, respectively. Both job postings included Derosier's contact information, including his cell phone number: (218) 399-2222.

On August 24, 2020, Rebecca Peterson called Detective Buzzo to lodge a complaint against Defendant after she was referred to him by the Consumer Protection Agency. Peterson reported that she had previously been defrauded by Defendant and that she had knowledge that he was currently doing business in Grand Forks. In particular, she observed Defendant's company vehicles and equipment at a worksite at the High Plains Court condo development in Grand Forks.

Continuing on August 24, 2020, Detective Buzzo drove to the High Plains Court condo development identified by Peterson. Detective Buzzo later determined that the Defendant was performing work at two condos owned by Ruth Ann Halvorson and Raymon Holmberg. Although Detective Buzzo did not observe any workers at the jobsite, he did observe certain equipment and materials such as bricks, lumber, and a dirt pile. He also observed that the projects at the worksite were unfinished.

Detective Buzzo later called the City of Grand Forks Inspections Office and spoke with Beverly Collings, the Building and Zoning Administrator. Collings relayed to

Detective Buzzo that the owner of one of the condos, Ruth Ann Halverson, had lodged a complaint against Defendant. Collings visited the jobsite to speak with Halvorson and later discovered that Defendant failed to obtain building permits for either Halvorson's or Holmberg's property. Collings also confirmed that neither Team Lawn, Inc. nor Derosier Outdoors was licensed to conduct business in Grand Forks.

Detective Buzzo later interviewed Halvorson, who stated that she previously contracted with Defendant's company to replace her patio and that he was also performing similar work at her neighbor Raymon Holmberg's property. Halvorson also told Detective Buzzo that Defendant had recently completed like work at another property also owned by her.

On August 25, 2020, Detective Buzzo drove to the condo development where Halvorson and Holmberg resided. Upon his arrival, Detective Buzzo observed Defendant's pickup parked at 621 High Plains Court, and several people working at the jobsite. Detectives Buzzo and Darin Johnson spoke with Shawn Halvorson, Blake Thoreson, and Christyan Logan, all of whom identified themselves as employees of Defendant. All three men told the Detectives that Defendant paid them for their work via check and that Defendant used QuickBooks, an accounting software, on his home computer. Using his phone, Logan showed Detective Buzzo a digital copy of his paystub which the Detective immediately identified as a QuickBooks template. Logan's payroll stub also revealed that Defendant used the business name of Garden & Patio HQ, Derosier Outdoor with an address of 412 5th Avenue South, Grand Forks, North Dakota.

Soon thereafter Defendant arrived at the jobsite. Detective Buzzo asked Defendant about his business, licensing, and the Order of Injunction & [Order] To Comply issued on October 15, 2019. Defendant claimed, among many things, that he was not properly served with the Order. He also told Detective Buzzo that "the entire case was a farce." Defendant explained that he was operating under a different business name. He stated the new business "took over for Team Lawn." During this same interview, Detective Buzzo observed that Defendant had a cell phone on his person. Upon questioning, Defendant told Detective Buzzo that his cell phone number was (218) 399-2222, and that his phone number was also listed on his GPHQ, LLC website as well as in advertisements for Team Lawn.

Following his conversation with Defendant, Detective Buzzo contacted the North Dakota Attorney General's Consumer Protection and Antitrust Division to verify Garden & Patio HQ, LLC's information. Detective Buzzo spoke with the Director of the Division who informed him that Garden & Patio HQ, LLC was not a licensed business in the state of North Dakota. Detective Buzzo also reviewed GPHQ, LLC's initial paperwork filed with the North Dakota Secretary of State, and discovered the business was registered on August 15, 2019, under the name of "Nicholas J. Derosier" with an address of 412 5th Ave. S., Grand Forks, ND 58201. The Secretary of State's Office also confirmed that GPHQ, LLC was not a licensed business in North Dakota.

Thereafter, Detective Buzzo spoke with Jack Hirst and Andrew Fox, former employees of Team Lawn, Inc. Hirst informed Detective Buzzo that he contacted the North Dakota Attorney General's Office because Defendant had failed to pay him for his

work. Hirst stated that he started working for Defendant in May 2019, and that he owed Hirst approximately $2,000 for his labor.

Detective Buzzo also spoke with former employee, Andrew Fox, who stated that he worked for Defendant's Team Lawn, Inc., from August 2018 to October 31, 2019. Fox explained that he filed a small claims case against Defendant for failure to pay wages. Fox told Detective Buzzo that Defendant operated his business out of his residence located at 412 5th Avenue South in Grand Forks. He further stated that Defendant had two computers at the residence, one of which he used for paying bills, bookkeeping, and drafting payroll checks with QuickBooks software.

Detective Buzzo reviewed Defendant's reply to Fox's small claims complaint, dated November 22, 2019, wherein Defendant represented that Fox was employed by Team Lawn, Inc. during certain dates that followed the District Court's Order precluding him from engaging in any business. Detective Buzzo obtained records for Defendant's business account from United Valley Bank. These records revealed that checks were deposited into the business account after October 15, 2019, some of which included notes for invoice numbers and notations from customers "paid in full." According to these same records, the GPHQ, LLC account was closed in March 2020, but Defendant continued to issue checks on the account. Specifically, on August 17, 2020, and July 20, 2020, he issued checks payable to Strata, Corp. and Hebron Brick respectively, two local businesses that supply landscaping materials.

Detective Buzzo also discovered a website for Garden & Patio Headquarters, LLC located at https://www.gardenpatiohq.com/. The website advertised that Garden & Patio

offered certain services such as landscaping, hardscapes, tree services, deck/patio construction, irrigation systems, custom outdoor spaces, fences, and snow removal services. The website included the following email address and cellular number for the business: gardenpatiohq@gmail.com and (218) 399-2222. Defendant acknowledged that this cellular number belonged to him when he was interviewed by Detective Buzzo on August 25, 2020.

On September 15, 2020, Detective Buzzo obtained and executed a North Dakota state search warrant for Defendant's person and his residence located at 412 5th Avenue South, Grand Forks, North Dakota. The search warrant authorized law enforcement to search and seize any files containing evidence of the crimes of contractor license required, construction fraud, and violation of a judicial order in any form wherever they may be found.

Because Homeland Security Investigations (HSI) Special Agent (SA) Dan Casetta was assigned to investigate white collar crime, he was invited to participate in the execution of the search warrant. As the only forensic examiner at the Grand Forks Police Department, Detective Jennifer Freeman was also invited to participate in the execution of the search warrant. Other local police officers participated in the search as well.

During the search of the business and residence, law enforcement seized a computer in Defendant's bedroom as well as several electronic storage devices including thumb drives and cellular phones in a safe also located in Defendant's bedroom. In addition, law enforcement seized a desktop computer with an attached thumb drive from

a desk on the main floor of the residence. And finally, a detective seized a black Android cellular phone from Defendant's person.

Continuing on September 15, 2020, Detective Freeman began to search the electronic devices. She first searched the 2GB Lexar thumb drive recovered from a safe in Defendant's bedroom. During a preliminary search of this device, she located files containing child pornography that were located in a folder entitled "Mega." As soon as she discovered these files, Detective Freeman immediately ceased searching the devices and sought a second North Dakota state search warrant.

On September 16, 2020, Detective Freeman applied for a North Dakota state search warrant to search the above-mentioned electronic devices for evidence of child pornography and exploitation. Detective Freeman analyzed several of the devices during which time she recovered thousands of child pornography files. She was not able to conduct a forensic examination of the Android cellular phone found on Defendant's person because it was encrypted. It would take law enforcement more than one year to gain access to this device.

Eventually, all of the electronic devices seized from Defendant's residence were provided to the North Dakota Bureau of Criminal Investigation (NDBCI) SA Jesse Smith for forensic examination. His forensic examination of the media revealed thousands of video and image files of child pornography as well as numerous conversations between Defendant and others during which time Defendant sent child pornography files. During some of these chat conversations, Defendant disclosed that he was sexually abusing two prepubescent-age boys.

Law enforcement continued to investigate Defendant's distribution of child pornography. Law enforcement later learned that Defendant traveled to Minnesota to meet with Justin Langen, a like-minded individual. During this meeting, Defendant showed Langen images of child pornography that Defendant claimed to have produced. Defendant further represented to Langen that he had immediate access to these children and would bring them to Caledonia, Minnesota, for the purpose of sexually abusing them. Defendant's cellphone includes chat and text conversations between Defendant and Langen that corroborate their meeting for this purpose.

B. National Center For Missing and Exploited Children CyberTips

After child pornography was discovered on Defendant's devices, law enforcement was able to connect Defendant to previous National Center for Missing and Exploited Children (NCMEC) CyberTips, one of which was previously investigated by HSI and the Grand Forks Police Department. On January 12, 2019, prior to the above fraud investigation of Defendant and his business, the Internet Crimes Against Children Task Force forwarded Detective Freeman a CyberTip. According to the CyberTip, Google discovered child pornography in a user's Google Photos infrastructure. Other than a telephone number, there was no identifying information about the user in the Cybertip. Detective Freeman reached out to HSI SA Mike Arel who was then assigned to the Internet Crimes Against Children Task Force (ICAC) for assistance in identifying the phone's user. SA Arel eventually determined that this number was owned by Midcontinent Communications and assigned to a landline (fixed VOIP), but had been ported to Verizon Wireless Communications.

Thereafter, SA Arel served a summons on Verizon Wireless requesting subscriber information for the telephone number. On February 23, 2019, Verizon Wireless responded to the aforementioned summons and indicated the subscriber for the target number was Sandra Simmons in Champlin, Minnesota. Verizon Wireless also provided that there was a secondary contact for the phone number; namely, Team Lawn, in Grand Forks.

On February 26, 2019, Detective Freeman discovered that Team Lawn was owned by Robert Coons and Defendant. Coons owned the residence located at 412 5th Avenue South in Grand Forks, where both Defendant and Coons resided and operated their business. During SA Arel and Detective Freeman's investigation, they learned that Robert Coons was killed in a skid steer accident on February 9, 2019. SA Arel and Detective Freeman also discovered that following the death of Coons, Defendant reported a burglary of his residence on February 19, 2019, where Coons also resided prior to his death. Defendant reported that certain electronic devices were taken from an upstairs room that was used for the Team Lawn business. During his report of this burglary, Defendant also told the GFPD that there was a prior unreported burglary of his residence that he claimed occurred one week prior to the February 19, 2019, burglary. The burglaries were investigated by the GFPD; however, no additional information was received and the investigations were later closed. Because SA Arel and Detective Freeman suspected that the CyberTip was most likely involving Coons, they closed their investigation.

More than fifteen months later, the Eagan Police Department (EPD) notified GFPD on July 13, 2020, that it had executed a search warrant of Justin Langen's residence in Hokah, Minnesota. As part of that investigation, the EPD discovered a chat conversation between Langen and Defendant on Langen's phone wherein they discussed their sexual attraction to prepubescent boys. This lead was eventually forwarded to Detective Freeman for further investigation, but she ultimately determined that their chat was not illegal. Then, in September 2020, Detective Freeman participated in the above-mentioned search warrant of Defendant's residence, but it was not until after Detective Freeman discovered the child pornography on Defendant's devices that she and SA Arel realized that the 2019 CyberTip was almost certainly involving Defendant. SA Smith was later able to connect Defendant to this and other CyberTips, including one that was assigned to law enforcement in South Dakota.

Law enforcement also eventually discovered that at least one of the computers that Defendant had reported as stolen from his residence during the February 19, 2019, burglary was seized by law enforcement during their search of the residence on September 15, 2020. Moreover, law enforcement discovered, albeit months later, that Defendant had added his name to at least one of Coons' accounts the day following his death and subsequently made charges to such account. Defendant added his name to other Coons' accounts in the ensuing months following his death. In other instances, Defendant assumed Coons' identity to make charges on certain other of Coons' accounts.

III. ARGUMENT

The defendant makes several arguments that the warrant was deficient. He argues that the warrant did not allege the items to be seized or the defendant's alleged offenses (it did), and that the warrant was not sufficiently "particular" with respect to time and file-type (it was), and that officers did not act in good faith in executing the warrant (they did). These arguments are addressed in turn below.

A. The Warrant Adequately Alleges the Place to be Searched and the Items to be Seized.

The warrant in this case specifically stated the items to be seized, and therefore no "magic words" of incorporation were necessary. Although the warrant contained a clerical error with respect to the place to be searched, the Eighth Circuit has considered that specific clerical error and has held that such an error is not fatal to the search warrant. These issues are considered in turn.

(1) The Warrant Set Forth, in Detail, the Items to be Seized, so it was not Necessary to Expressly Incorporate the Affidavit

The Fourth Amendment provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. "The particularity requirement can be satisfied by listing the items to be seized in the warrant itself *or* in an affidavit that is incorporated into the warrant." United States v. Szczerba, 897 F.3d 929, 937 (8th Cir. 2018) (emphasis added). See also United States v. Sierra, 2022 WL 2866371, at *2 (D.S.D. July 21, 2022) ("The Eighth Circuit has recognized that

the Fourth Amendment's particularity requirement can be satisfied by including the items to be seized in the warrant *or* in an incorporated document") (emphasis added).

Here, the warrant listed the items in detail on the face of the warrant itself, so no incorporation of the affidavit was necessary. Specifically, Attachment 2 – Search Warrant Attachment A which was attached to the warrant contained a "DESCRIPTION OF ITEMS TO BE SEARCHED FOR AND SEIZED," which provided the following:

> By forensic or other means of examination: Files containing evidence of the crimes of Contractor License Required, Construction Fraud, and Violation of a Judicial Order in any form wherever they may be stored.
>
> Portable electronic devices capable of storing files related to the aforementioned crimes. Such items include, but are not limited to, cellular telephones, iPads, iPods, tablet computers, notebook computers and netbook computers.
>
> Information, correspondence, records, documents or other materials pertaining to the possession, receipt or distribution of visual depictions of projects, job sites, communications, account data, timesheet information, customer information, address, and accounts that were transmitted or received using the digital media, including, but not limited to: electronic mail, chat logs, and electronic messages or any other forms of transmission.
>
> Records evidencing ownership of digital media devices and removable storage, to include; evidence of who used or controlled the computer at the time the items described in this warrant were created, edited, or deleted, such logs, registry entries, saved usernames and passwords, documents, and browsing history; Evidence of software that would allow others to control the computer, such as, viruses and other forms of malicious software; Evidence of the attachment to the computer of other storage devices, disks, or similar containers; Evidence of the times the computer was used, passwords, encryption keys, and other devices that may be necessary to access the computer.
>
> Any computer, computer system and related peripherals; tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic

> media floppy disks, hardware and software operating manuals, tape systems and hard drive and other computer related operation equipment, digital cameras, scanners, computer photographs, Graphic Interchange formats and/or photographs, undeveloped photographic film, slides, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG), and any electronic data storage devices including, but not limited to hardware, software, diskettes, backup tapes, CD-ROMS, DVD, Flash memory devices, and other storage mediums; any input/output peripheral devices, including but not limited to passwords, data security devices and related documentation, and any hardware/software manuals related to or used to: contain information pertaining to the use of the computers or other electronic devices for storing, facilitating, and/or drafting payroll accounts, customer accounts, estimates, statements, and other business documents.

Attachment 2 – Search Warrant Attachment A. Because the warrant itself is clear with respect to the items to be seized, the Court can and should stop there.

The concept of incorporation is thus a red herring here, and the two cases defendant cites are inapposite. In United States v. Szczerba, 897 F.3d 929, 937 (8th Cir. 2018), "[t]he warrant lacked particularity because it did not list the items to be seized ***or*** incorporate" the affidavit. Id. (emphasis added). Here, the warrant did list the items to be seized, so there was no need to use express words of incorporation. In United States v. Curry, 911 F.2d 72, 76 (8th Cir. 1990), the Court held the warrant was not particular because it "did not identify the premises to be searched because the space for filling in that information was left blank," and also because the warrant did not expressly incorporate the affidavit. Id. Here, the space for the premises to be searched was not "left blank," but rather, stated "on or within the person known as Nicholas Derosier a/k/a Nicholas Morgan-Derosier, presently located at 412 5th Ave S, Grand Forks, ND 58201."

Finally, although the Defendant cited several other cases for the proposition that express incorporation language is necessary, the Eighth Circuit has been far from clear on that proposition. United States v. Weber, 346 F. Supp. 3d 1335, 1343 (D.S.D. 2018), aff'd, 987 F.3d 789 (8th Cir. 2021) ("this area of law in the Eighth Circuit on incorporation of other documents in a search warrant is both 'questionable' and 'thorny.'"); see United States v. Gamboa, 439 F.3d 796, 807 (8th Cir.2006) ("[A]n affidavit may provide the necessary particularity for a warrant if it is either incorporated into *or attached to the warrant*." (quoting Rickert v. Sweeney, 813 F.2d 907, 909 (8th Cir.1987)) (emphasis added); United States v. Nieman, 520 F.3d 834, 839 (8th Cir. 2008) ("An affidavit may provide the necessary particularity for a warrant if it is incorporated into the warrant, *attached to the warrant, or present at the search*.") (emphasis added). Because the warrant is sufficient on its own, however, the court need not necessarily decide this issue. But United States notes that this issue appears to be an open one in the Eighth Circuit.

In short, because the warrant, on its face expressly listed, in detail, the items to be seized, the warrant did not need to expressly incorporate the affidavit.

(2) The Warrant's Language that Provided for a Search "on or within the person known as Nicholas Derosier presently located at 5th Ave S, Grand Forks, ND 58201" was an Excusable Clerical Error.

The warrant's clear intent was to authorize a premises search, not just a search of Defendant's person. The intent is evident for at least two reasons. First, the affidavit expressly seeks a premises warrant *and* a warrant search of Derosier's person:

> Your affiant believes probable cause exists that Nicholas J. Derosier a/k/a Nicholas Morgan-Derosier has committed the crimes of Violation of a Judicial Order and Contractors License Required, and Construction Fraud and *evidence of those crimes are contained within the computers and other electronic communication devices within 412 5th Ave S*, and Derosier's cellular telephone. Your affiant requests a search warrant be issued authorizing your affiant to search for and seize the computers and other electronic communication devices, electronic storage devices such as the computer's hard drive, removable media such as, CDs, DVDs, or portable flash (USB) drives, and the like. Additionally, your affiant requests the search warrant to allow him to search Derosier's person and *seize his cellphone if it is not found during the search of the residence*. Additionally, your affiant requests the search warrant to authorize a search and forensic examination of all seized computers, electronic communication, and storage devices found and seized under this warrant . . . .

Attachment 2 - Affidavit at ¶ 22 (emphasis added). The request to search Defendant's person was only for his cell phone, and only to the extent officers did not recover it from the premises search. The affidavit also contains multiple other paragraphs describing facts that relate to Morgan-Derosier's use of his address to conduct his lawn business. Attachment 2 – Affidavit at ¶¶ 8, 9, 11, 16, and 22.

Second, common sense dictates that items of which the warrant authorized seizure would very likely be found in a premises search, but would be exceedingly unlikely to be found on Defendant's person. Specifically, the warrant authorized the seizure of, *inter alia*:

- correspondence, records, documents or other materials pertaining to the possession, receipt or distribution of visual depictions of projects;
- Any computer, computer system and related peripherals; tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, **monitors, computer printers, modems,** tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and **hard drive and other computer related operation equipment**, digital cameras, **scanners**, computer photographs,

- electronic data storage devices including, but not limited to hardware, software, diskettes, backup tapes, CD-ROMS, DVD, Flash memory devices, and other storage mediums;
- **hardware/software manuals** related to or used to contain information pertaining to the use of the computers or other electronic devices for storing, facilitating, and/or drafting payroll accounts, customer accounts, estimates, statements, and other business documents.

Most of these items are infrequently in anyone's physical possession after they are initially installed in one's house (monitors, printers, modems, other computer hardware, hard drives, all of one's paper business records, etc.) But more significantly, it is all but impossible for *all* of those items to be in a single person's physical possession *at one time* and *at the exact moment officers execute the search warrant*.

This is not a case where the warrant sought, for example, a single cell phone that a defendant might be just as likely to possess, at any one time, on one's person or in one's house. In that case, it would be more difficult to discern whether the court intended to authorize the search of a single person and not a premises intentionally. This is also not a case of a post-hoc rationalization for improper law enforcement search. Here, the affidavit expressly sought, and the warrant authorized, the search and seizure of a large amount of physical hardware and digital business records that would be exceedingly unlikely or impossible for anyone to physically possess on his person at any one time. In short, people do not carry printers in their pockets.

The exclusionary rule does not apply here because the intent of the Court was clear. The Eighth Circuit Court of Appeals has opined on essentially the same clerical error in Szczerba, and held that the exclusionary rule did not apply under the circumstances:

> We first conclude that the warrant's authorization to search "said person" instead of "said property" did not render the warrant invalid. The warrant particularly described the hotel room and the Mercedes. The omission of the word "property" from the authorizing language appears to be a clerical error in light of the warrant's meticulous identification of the hotel room and the Mercedes, the affidavit's similarly meticulous description and its request to search the hotel room and the Mercedes, and the warrant's otherwise nonsensical authorization of the seizure of "above described property" (*i.e.*, the hotel room and the Mercedes) if it "be found on the said person by you." In these circumstances, a reasonable officer executing the warrant likely would have read the warrant to authorize the search of the particularly described property and not the person who was mentioned only in relation to the property and only because the property was registered in her name.

Szczerba, 897 F.3d at 936–37; See also United States v. Weber, 346 F. Supp. 3d 1335, 1344 (D.S.D. 2018), *aff'd,* 987 F.3d 789 (8th Cir. 2021) ("The United States Court of Appeals for the Eighth Circuit recently reviewed a search warrant involving facts very similar to this case. In Szczerba, the court held 'that the warrant's authorization to search 'said person' instead of 'said property' did not render the warrant invalid.'") Similarly, here, the affidavit meticulously articulated a basis to search Defendant's premises. Therefore, the officers relied on the warrant in good faith when they searched defendant's property.

B. The Warrant Properly Alleges Several Specific Crimes.

Defendant's next argument, namely, that "[t]he warrant[1] did not identify what crime was alleged to have been committed," Doc. 70-01 at 16, need not detain the court

[1] Again, it is worth noting that it is an open legal issue in the Eighth Circuit whether this court can consider both the warrant and affidavit, but because the warrant itself is sufficient by itself here, the Court need not decide that issue. See United States v. Weber, 346 F. Supp. 3d 1335, 1343 (D.S.D. 2018), aff'd, 987 F.3d 789 (8th Cir. 2021) ("this area of law in the Eighth Circuit on incorporation of other documents in a search warrant is both 'questionable' and 'thorny.'"); see United States v. Gamboa, 439 F.3d 796, 807 (8th Cir.2006) ("[A]n affidavit may provide the

long because it is not a factually accurate statement. "Indeed, it is not necessary for an affidavit to include the name of the specific crime alleged. Rather, only a probability of criminal conduct need be shown." United States v. Alexander, 574 F.3d 484, 489 (8th Cir. 2009) (quoting United States v. Summage, 481 F.3d 1075, 1078 (8th Cir.2007)). "The fourth amendment . . . requires only that the warrant particularly describe the place to be searched, and the persons or things to be seized; neither the fourth amendment nor our holdings require particularity with respect to the criminal activity suspected." United States v. Horn, 187 F.3d 781, 787 (8th Cir. 1999). "It is not necessary for an affidavit to include the name of the specific crime alleged." United States v. Summage, 481 F.3d 1075, 1078 (8th Cir. 2007).

Here, the warrant and affidavit not only articulate the criminal conduct in general terms, which is all that is required, but they both goes even further. The warrant lists three crimes by their proper names. Specifically, the warrant authorizes the government to search for "[f]iles containing evidence of the *crimes of Contractor License Required,*[2]

---

necessary particularity for a warrant if it is either incorporated into *or attached to the warrant*." (quoting Rickert v. Sweeney, 813 F.2d 907, 909 (8th Cir.1987)) (emphasis added); United States v. Nieman, 520 F.3d 834, 839 (8th Cir. 2008) ("An affidavit may provide the necessary particularity for a warrant if it is incorporated into the warrant, *attached to the warrant, or present at the search*.") (emphasis added)

[2] The text of the statute entitled "License Required – Construction Fraud" provides:

1. A person may not engage in the business nor act in the capacity of a contractor within this state when the cost, value, or price per job exceeds the sum of four thousand dollars nor may that person maintain any claim, action, suit, or proceeding in any court of this state related to the person's business or capacity as a contractor without first having a license as provided in this chapter.

2. Any person acting in the capacity of a contractor without a license is guilty of a class A misdemeanor. Regardless of whether a person is subjected to criminal prosecution under this subsection, and in addition to the license fee that may be assessed when the person applies for a license, the person may be assessed a civil penalty by the registrar, following written notice to the

Construction Fraud,[3] *and Violation of a Judicial Order*[4] in any form wherever they may be stored." Warrant, Attachment 2 (emphasis added). The affidavit similarly alleges, in paragraph 22, that "Your affiant believes probable cause exists that Nicholas J. Derosier a/k/a Nicholas Morgan-Derosier has committed the crimes of Violation of a Judicial

---

person of an intent to assess the penalty, in an amount not to exceed three times the amount set forth in section 43-07-07. Any civil penalty must be assessed and collected before a person is issued a license. The assessment of a civil penalty may be appealed in the same manner as appeals under section 43-07-04.

N.D.C.C. § 43-07-02(1)(2).

[3] The text of the construction fraud statute continues:

A person commits construction fraud if:

a. The person receives payment for a construction project by intentionally using deception as defined in section 12.1-23-10.

b. The person receives payment for the purchase of materials or supplies and willfully fails to pay the supplier for the goods received.

c. The person willfully abandons a construction project after receiving payment for services or materials. Abandonment under this subdivision arises if:

(1) A contractor fails substantially to commence any work agreed upon:

(a) Within sixty days of a starting date agreed upon in writing; or

(b) Within ninety days of the contract date if no starting date is agreed upon in writing; or

(2) A contractor fails to complete any work agreed upon in writing within ninety days of a completion date agreed upon in writing, or within one hundred eighty days of the contract date if no completion date is agreed upon in writing.

N.D.C.C. § 43-07-02(3).

[4] The text of the statute entitled "Disobedience of Judicial Order" provides:

1. A person is guilty of a class A misdemeanor if the person disobeys or resists a lawful temporary restraining order or preliminary or final injunction or other final order, other than for the payment of money, of a court of this state.

2. Notwithstanding the limitations of section 12.1-32-01, the defendant may be sentenced to pay a fine in any amount deemed just by the court.

N.D.C.C. § 12.1-10-05.

Order and Contractors License Required, and Construction Fraud." Id.; see N.D.C.C. § 12.1-10-05 ("Disobeying a Judicial Order"); 43-07-02(1) and (2) ("License Required – Construction Fraud."). So, the defendant's assertion that "[t]he warrant did not identify what crime was alleged to have been committed," Doc. 70-01 at 16, is factually false.

And the defendant knows it is false because he relegates, to a footnote, an "acknowledgment" that the warrant *does* in fact identify the specific crimes by name, but that it in essence does not "count" because (he believes) it should have been listed in a different place in the warrant. That argument is form over substance, and the defendant fails to cite any legal authority for applying the exclusionary rule to a warrant because it was not organized properly.

C. The Defendant's Argument that the Warrant did not Limit the Search Based on File Created Dates is without Merit Because the Warrant Limited the Search to Specific Crimes.

"To satisfy the particularity requirement of the fourth amendment, the warrant must be sufficiently definite to enable the searching officers to identify the property authorized to be seized." United States v. Summage, 481 F.3d 1075, 1079 (8th Cir. 2007) (citing United States v. Horn, 187 F.3d 781, 788 (8th Cir. 1999)). "The degree of specificity required will depend on the circumstances of the case and on the type of items involved." Id. (citing Horn, 187 F.3d at 788). The particularity requirement required under the Fourth Amendment is not a "hypertechnical" standard, but one of "practical accuracy." Id. (citing United States v. Peters, 92 F.3d 768, 769–770 (8th Cir.1996)); United States v. Sherman, 372 F. App'x 668, 675 (8th Cir. 2010). We consider "the purpose for which the warrant was issued, the nature of the items to which it is directed,

and the total circumstances surrounding the case." United States v. Fiorito, 640 F.3d 338, 346 (8th Cir. 2011) (quoting Milliman v. Minnesota, 774 F.2d 247, 250 (8th Cir. 1985)).

"Inclusion of a statutory reference can sufficiently limit the scope of a search and thus provide the necessary particularity." United States v. Dockter, 58 F.3d 1284, 1288 (8th Cir. 1995) (citing Rickert, 813 F.2d at 909). "A warrant naming only a generic class of items may suffice if the individual goods to be seized cannot be more precisely identified at the time that the warrant is issued." United States v. Horn, 187 F.3d 781, 788 (8th Cir. 1999).

The circumstances of this case show that the warrant here was properly limited to specific crimes. The warrant itself listed three offenses in the warrant– Contractor License Required, Construction Fraud, and Violation of a Judicial Order – and the affidavit included several dates when operative facts occurred. It is unclear how much more "particular" the warrant could even have been. It would be impossible to know, for example, the identity of all the specific devices on which the defendant saved illegal documents, or the specific filenames that showed he was running a landscaping business before officers searched for those items. Because the warrant is limited in scope to specific offenses, the warrant is sufficiently particular. Dockter, 58 F.3d at 1288 (citing Rickert, 813 F.2d at 909); See also United States v. Christie, 717 F.3d 1156, 1165 (10th Cir. 2013) (holding that warrants "may pass the particularity test if they limit their scope either to evidence of specific federal crimes or [to] specific types of material.") Again, the Court can and should stop there.

Although the Court need not, and should not, get further "into the weeds," the defendant's specific assertions fail on their own merit too, so the United States will brief those issues for completeness. In his memo defendant argues that (1) there could be no evidence prior to October 15, 2019 (the day he lost his business license) related to prior landscaping businesses that might bear relevance to him continuing landscaping businesses after that date;[5] and (2) the warrant can and should specifically direct the government to (somehow) filter devices for files that have created dates that postdate October 15, 2019. Those arguments are considered here out of an abundance of caution, should the Court reach them.

(1) Evidence of Business Activity Prior to October 15, 2019, bears possible Relevance to Show Defendant Continued Landscaping Businesses After that Date.

Any documents that show the defendant's landscaping business practices both before and after he lost his license would be potentially relevant to establish that he continued to engage in landscaping. The defendant was not, for example, alleged to have *started* his first new landscaping business on October 15, 2019, but instead was alleged to have continued to run landscaping businesses after that date.[6] So the nature and conduct of the defendant's landscaping businesses both before and after that date would be at least

[5] Doc. 70-1 at 17 ("Det. Buzzo was investigating Mr. Morgan-Derosier for operating a business after he was allegedly forbidden from doing so in an order dated 15 October 2019. The crime, therefore, could not have occurred before 15 October 2019. . . . Thus, the warrants allowed officers to seize years' worth of records which had nothing to do with whether Mr. Morgan-Derosier had committed a crime after 15 October 2019.")

[6] Even if the defendant did start a business on October 15, 2019, evidence of his conduct, communications, and finances prior to starting the business would be relevant to show his intent on the date he started his business.

potentially relevant to prove that his conduct after October 15, 2019, was consistent with landscaping. For example:

- Emails with employees, customers and suppliers, saved contacts and calendars prior to October 15, 2019, would be relevant to establish a baseline of business activity that would explain why contacts, communications, meetings, appointments, etc. after that date were business related and not personal;

- Receipts, invoices, bank records, accounting records, and other financial information prior to October 15, 2019, would be similarly relevant to show Defendant's income after that date was derived from his unauthorized business, and that expenses were incurred from the business and not his personal life;

- Equipment purchases and other capital expenditures prior to October 15, 2019, would be relevant to explain why he purchased, or did not need to purchase, landscaping or other business equipment after October 15, 2019;

- Original incorporation documents, mission statements, and communications prior to October 15, 2019, would be relevant to prove he continued the same business after that date.

These are just a few examples, but it would be difficult to imagine a document related to his business prior to October 15, 2019, that would be wholly irrelevant to show he continued the same business after that date.

Of course, what is ultimately seized, and what is authorized to be searched, are two different questions. Moreover, officers in this case did not seize all the paper records that *could* have been relevant, and for which there was probable cause to seize. In fact, it is the best practice for officers to exercise discretion with respect to which devices and which records they seize during the execution of a search warrant, even if there is some small chance that it may miss some relevant evidence, or even if officers know of the relevance but it is only tangentially relevant or duplicative. In short, officers must triage.

Seizing, for example, hundreds of "tera-bytes" of data, or every piece of paper in every case would cause the government (and the defendant, after criminal discovery) to spend substantial time and resources to process and review all the data. Exercising the discretion not to seize a device or a record, even though one has probable cause to search or seize that particular device or record, however, does not render the search warrant "overbroad." Triage during searches is standard practice.

But more broadly, other computer files on devices prior to October 15, 2019, are relevant to prove identity, namely, that the Defendant was the one who was running his business after that date. Regardless of when a document was created, the document itself – a resume, a family photo, numerous "selfies," letters and correspondence, etc. – can show that the defendant was, or was not, the exclusive user of the computer that conducted the unauthorized business, or engaged in construction fraud.

Instead, Courts hold that the more reasonable limiting principal for a search is not always a specific date range, but an allegation of a specific crime. United States v. Dockter, 58 F.3d 1284, 1288 (8th Cir. 1995) (citing Rickert, 813 F.2d at 909). Like in this case, a specific date range of relevant evidence is difficult or impossible to determine. Therefore, in those cases limiting the search by allegation is appropriate.

(2) Searching for and Seizing only files that Were Created After a Certain Date is a Impractical and is Not Legally Required.

"The requirement of particularity must be assessed in terms of practicality." United States v. Summage, 481 F.3d 1075, 1079 (8th Cir. 2007); (quoting United States v. Hill, 459 F.3d 966, 974-75 (9th Cir. 2006); United States v. Upham, 168 F.3d 532, 535

(1st Cir.1999); and United States v. Horn, 187 F.3d 781, 788 (8th Cir. 1999)) For example, "[a]n off-site analysis of the relevant materials is therefore often necessary" because the warrant's particularity must be viewed in terms of practicality. Summage, 481 F.3d at 1079.

Here, limiting a "search" of a device to files with a specific type of content, or a specific date range, is neither legally required, nor practicable. An analogy is helpful. Searching a hard drive is akin to searching a sealed package. If a dog alerts to the presence of cocaine in a sealed package, for example, the law enforcement officer could obtain a valid search warrant for the entirety of the package even though some items inside the package might not be illicit. The officer must search the whole package, and all of its contents, to make sure he finds all the cocaine in it. The sealed container might contain a brick of cocaine and a dictionary. It may contain a brick of cocaine and a brick of heroin. As a legal matter, the potential presence of non-illicit materials, or even other different illicit materials, does not render a search warrant for the entire package overbroad. And as a practical matter, there would be no realistic way to limit the search of the sealed package to only cocaine, or only certain compartments of the package. In fact, one of the very purposes of the search is, necessarily, to sort the legal from the illegal.

Similarly, in the computer context, there would be no way to determine whether a file folder labelled "documents," for example, contained illicit files unless officers, at a minimum, opened the folder and looked at the files. But further, if there was a Word document located in that "documents" file labelled ABC123.doc, there would be no way

to determine whether that file was a grocery shopping list, a school project, or a drug ledger without opening the file. Defendants rarely label their file folders "illegal business documents," or their Word documents as "contract-for-lawn-services-after-I-lost-my-business-license.doc." And even if they did, discovery of those folders and files would not "end" the search for other business-related documents.

A hard drive that contains computer files is like a sealed package. If there is probable cause to search a hard drive for evidence of a crime, officers should search the entire device for evidence of specifically-enumerated offenses – the limiting principal.

Defendant's proposed proxy to somehow filter by "file creation date" is not practical for several reasons. First, defendant's proposal presupposes a search of the entire device to begin with. Specifically, to compile and export files by file creation date, the forensic technician would need to hash and image the device (the whole thing), and run a software that sorts files using meta-data. There is no "automated" way to sort all the files and reliably ensure there is an exhaustive list of files created after a certain date – a forensic technician would need to check those things. Defendant would likely agree dumping an entire device and sorting it by meta-data is, in fact, a search of the entire device. Moreover, some "database" files – like email .pst files, for example – are not parsed by date automatically, so those would need to be sorted "by hand."

Second, some very important files do not have "file creation" dates at all. Deleted files are often the most important pieces of evidence to prove criminal conduct occurred because they can show consciousness of guilt. One reason why a defendant might delete an incriminating document or file is to avoid detection. Deleted files (which are

recovered from a computer's "unallocated space,") almost never have created dates. Moreover, to the extent defendant argues that all of this should occur "on scene," and that the government should only remove from the premises the offending files, the process for extracting deleted files from unallocated space can, depending on the device, takes a significant amount of time and requires technological equipment, so doing that "on-scene" would not necessarily be practical without "seizing" the defendant's entire house for long periods of time. Depending on the size of the digital media, imaging and "carving" can take many hours to several days. In addition to deleted files, thumbnail images of documents and pictures in a "thumbs.db" show the existence of files that a defendant may have viewed and saved, but later deleted to hide his conduct. Thumbnails also do not have file creation dates. So enforcing a "created date" limitation would prevent the potential discovery of highly relevant evidence.

Third, even if a file has a "file created date," the accuracy of that date relies, in turn, on the accuracy of the date and time settings of a computer, which can sometimes be wrong, and a user can also manipulate the file creation date. Moreover, a "file creation date" does not mean what the defendant purports it to mean, namely, the date a file first came into existence. Instead, "file creation date" is a term of art that generally refers to when a document is first "created" on a computer's operating system. That date is not necessarily the same date as the document came into existence anywhere in the world. For example, moving a file from a thumb drive to a hard drive might change the creation date of the file on the hard drive. In short, file created dates are not completely reliable to show when a file first came into existence.

Again, the Court need not reach these admittedly technical issues because the search warrant in this case properly limited the search to three alleged crimes. This is all to say that defendant's proposal to limit all computer searches by file creation date (1) lacks merit because there was likely to be highly relevant evidence on defendant's devices that was created prior to October 15, 2019, and (2) restricting a search by file creation date is not legally required or practical.

D. There was Probable Cause to Search the Defendant's Image Files

Defendant's next argument is that, in addition to using "file created dates" as a proxy for relevance, the Court should also use "file-type" as another proxy. The Eighth Circuit and other courts have rejected, repeatedly, similar file-type restriction arguments:

- See, *e.g.* United States v. Sherman, 372 F. App'x 668, 675–76 (8th Cir. 2010) ("Sherman claims the warrant should have been limited to a seizure of the Tracker Program, because Tracker was well known in law enforcement. Sherman fails to acknowledge he had access to all components of the computer system used in his business and that the computer data could be manipulated, stored in different formats, or stored outside of the Tracker Program.")

- United States v. Gleich, 293 F. Supp. 2d 1082, 1088 (D.N.D. 2003), aff'd, 397 F.3d 608 (8th Cir. 2005) ("Although Gleich contends that the . . . search warrant needed to more specifically list which computer files were to be searched, the search warrant clearly identified that the computers were to be searched for 'Photographs, pictures, visual representations, or videos in any form that include sexual conduct by a minor, as defined by N.D.C.C. 12.1–27.2–01(4).'")

- United States v. Summage, 481 F.3d 1075, 1079–80 (8th Cir. 2007) ("Because no indication was given regarding the nature of the format in which the sought-for video and photographs were created or stored, it was necessary to search a broad array of items for the relevant materials, the on-site search of which could take a significant amount of time.")

Again, the Court can and should stop there.

For completeness, however, the Defendant's argument fails on its own merits. He argues that the only type of computer file that could possibly be relevant to showing someone was engaged in landscaping is "Quickbooks accounting materials and other business-related lists and charts." (Doc. 70-1 at 20.) First, defendant's argument is without merit because lists and charts can easily be stored as image files. Second, and more importantly, it does not take much imagination to see how other file-types, including "image or video files," would be relevant to show he engaged in landscaping after he lost his license. For example, those files might depict:

- Images of invoices, receipts, spreadsheets, etc.
- Images or videos of job sites
- Images or videos of a landscaping office or office equipment
- Images or videos of customers
- Images or videos of employees
- Images or videos from customers complaining about how their grass was not properly mowed
- Images or videos of business-related travel to meetings and conferences.

It is common knowledge that pictures often show a person's typical daily activities and associations. A scroll through the undersigned's camera roll would quickly reveal that I am a lawyer for the Department of Justice. It includes pictures from my business office, the places I have had court hearings or other teaching engagements, the people with whom I practice (colleagues), etc. That evidence may not be enough, by itself, to show I was a lawyer for the Justice Department, but it would certainly be relevant evidence. Evidence need not be an entire wall to be relevant – it just needs to be a brick. Fed. R. Evid. 401 app. note. ("The standard of probability under the rule is 'more . . . probable

than it would be without the evidence.' Any more stringent requirement is unworkable and unrealistic. As McCormick §152, p. 317, says, "A brick is not a wall . . . .")

Defendant continues that "[n]owhere in his affidavit does Det. Buzzo explain or allege that business records are stored as image or video files." (Doc. 70-1 at 20.) That is not accurate. The affidavit provides:

> Computers have also revolutionized the way in which people can access and keep their records including personal, *business, and financial documents* and information. The development of computers and the Internet has greatly changed and added to the way in which people keep records. Computers have facilitated the ability of people to keep their records stored and hidden. *Photographs, videos, and other records* that were previously stored in boxes are now collected as *digital images and files* that can be stored and maintained on electronic media, such as a digital storage device called a "Micro Secure Digital Card," that is smaller than a postage stamp. Computers and the Internet now aid and serve in the storage of files and communication between people including customers.

Attachment 2 - Affidavit at ¶ 17 (emphasis added). Defendant's argument is thus without merit because there was probable cause to search images.

E. Defendant's Argument that Officers "Abandoned" a Specific Search and Engaged in a General Search is Similarly Without Merit.

This is the quintessential example of a case in which the officers did *not* abandon a search, authorized by a warrant, in favor of another search. If an officer is executing an otherwise lawful search and finds evidence of a different crime and wants to continue his search for evidence of the new crime, he can go back and get a new warrant for the new crime. See United States v. Suing, 712 F.3d 1209, 1212 (8th Cir. 2013) (holding that a search was not improperly abandoned when, "[w]hile examining his computer [for evidence of drug dealing], authorities found images of child pornography. . . . [W]hen

officials found the images, they immediately stopped searching for evidence of illegal drug activity . . . and obtained a second warrant authorizing a search for child pornography.")

Here, officers did not "abandon" the business record search to search for child pornography search until *after* they obtained a warrant to search for child pornography. Specifically, shortly after officers began the forensic search of defendant's thumb drive, they found a folder labelled "Mega." Mega is a cloud-based storage application on which users can store and share documents and photos – such as business records. The forensic officer saw two files – "klein (33)" and "klein (35)." Not knowing what those files contained, the officer opened those files and viewed them as part of the authorized search for business-related files. Those files, however, contained images that depicted 7–9-year-old boys being orally raped by adult men. Officers stopped the search immediately at the sight of those images and obtained a search warrant for child sexual abuse materials, which was executed the following day. Officers literally did the opposite of abandoning a business-related search for a CSAM search without a warrant.

This may have been a closer call if, for example, after seeing images of little boys being raped, officers continued to look through defendant's devices for more business records. The court would then need to discern whether the officers really intended to obtain business records, or whether they were really searching for CSAM. But that did not happen here. Officers immediately sought a warrant before searching defendant's devices for CSAM – at the earliest possible opportunity.

Defendant argues that the opening of the "klein" files in the first instance was the abandonment of the search. That would only be true, however, if agents *knew* those files were not business related. As previously stated, however, it is impossible to know from a filename what the file actually contains without opening it. And even if officers were to trust that filenames are always conclusively indicative of file content, files labeled "klein" are certainly not necessarily indicative of the sexual abuse of a 7–9-year-old boy.

F. The Evidence Should Not Be Suppressed Because The Officers Who Executed The Search Warrant Acted in Good Faith and Reasonably Relied on the Warrant.

"Even if a court ultimately determines that a warrant approved by a judge falls short of the constitutional requirements of probable cause or particularity, evidence will not be suppressed if 'a law enforcement officer relies in objective good faith on a warrant issued by a detached and neutral magistrate.'" United States v. Cotto, 995 F.3d 786, 795 (citing United States v. Leon, 468 U.S. 897, 922 (1984)). When determining an officer's good faith reliance on a search warrant, this Court can look outside the four corners of the affidavit and consider the totality of the circumstances, including what the officer knew but did not include in the affidavit and warrant. United States v. Dickerman, 954 F.3d 1060, 1065 (8th Cir. 2020). There are only four circumstances that preclude a finding of good faith:

> (1) when the affidavit or testimony in support of the warrant included a false statement made knowingly and intentionally or with reckless disregard for its truth, thus misleading the issuing judge; (2) when the judge "wholly abandoned his judicial role" in issuing the warrant; (3) when the affidavit in support of the warrant was "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable," and

> (4) the warrant is "so facially deficient" that the executing officer could not reasonably presume the warrant to be valid.

United States v. Grant, 490 F.3d 627, 632-3 (8th Cir. 2007) (citing Leon, 468 U.S. at 923).

The defendant does not allege that Detective Buzzo made a false or misleading statement in the affidavit supporting the search warrant. Nor does he challenge the probable cause supporting the search warrant. Instead, he claims that the warrant is invalid because it does not include certain incorporation language in the warrant. In United States v. Weber, 346 F.Supp.3d 1335, 1344 (S.D. Oct. 15, 2018) the defendant made a similar argument.

The defendant in Weber claimed that the particularity requirement of the Fourth Amendment was not met because the warrant, which did not identify the property to be seized, failed to incorporate the affidavit and the attachments. The district court held that even if the warrant did not meet the particularity requirement for failure to incorporate the warrant, the facts of the case did not support suppression under the Leon good-faith exception because the application was referenced in the search warrant and accompanied the search warrant at the time the magistrate considered and signed the warrant.

Importantly, the agent submitted the affidavit and the warrant with attachments as a single bundle throughout the application and execution process. Id. at 1345. The Court also determined that the prosecutor's review of these same documents before they were submitted to the judge weighed in favor of applying the good-faith exception. "If there were any errors in any preparation of the documents, an objectively reasonable law

enforcement officer would expect [the AUSA] to point out those errors and make corrections prior to presentation of the packet to the magistrate judge." Id. at 1346. The court also recognized that the officer could have expected that the magistrate judge, after having reviewed the search warrant packet, would have notified the AUSA if she discovered any errors. Likewise, the court also determined that an objectively reasonable officer could expect the magistrate Judge to reject the search warrant or suggest corrections before executing the search warrant. Finally, after having obtained the warrant, the affiant, in an effort to limit the search, briefed the law enforcement officers on the case and directed the search. Based upon a totality of these circumstances surrounding the issuance and execution of the search warrant, the district court concluded that the officer's actions were objectively reasonable in believing the warrant, bundled together with the carefully construed supporting documents and authorized by a neutral magistrate judge, authorized the seizure of the items obtained from the defendant's residence. Id. at 1345.

Similarly, here Detective Buzzo was familiar with all of the information in the warrant and its supporting affidavit and attachments. Moreover, all of these documents that clearly identified the place and things to be searched and seized were presented to the Court together such that it was clear that Defendant's residence and person were the subject of the search. Detective Buzzo will testify that this same bundle of documents was also reviewed by an Assistant State's Attorney before he submitted it to the judge who likewise did not discover any errors in either the incorporation of the affidavit or the typographical error in the warrant. And after the judge signed the warrant, Detective

Buzzo had a meeting with the other officers who he invited to participate in the execution of the search warrant during which time he briefed all of the officers on the case and the scope of the search. He will even testify that some of these same officers reviewed the search warrant packet and he had it with him, as is his practice, when he executed the search warrant. Given these facts, it was objectively reasonable for Detective Buzzo to believe the warrant packet authorized him to search Defendant's person and residence for the items that were seized.

Despite Detective Buzzo's good-faith reliance on the warrant, Defendant claims that the good-faith exception is not available here because officers failed to execute the warrant within its scope. He argues they searched for child pornography rather than the specified crimes as authorized by the warrant. Again, as argued above, there is nothing here to indicate Detective Buzzo or any of the other officers abandoned the search for the crimes at issue in favor of a search for child pornography. All of the officers' actions demonstrate that they were focused on the search for the crimes as authorized by the warrant. For instance, the officers took photos of a white board at the residence which depict work projects and they also took photos of landscaping equipment in the yard. And when Detective Buzzo interviewed Defendant, it was only about his business. He did not ask any questions about the Cybertip or child pornography. The fact that Detective Freeman later found child pornography on one of the devices does not indicate differently. To the contrary, her actions—ceasing the search of the devices upon the discovery of child pornography and obtaining a second search warrant—reveal she was aware of the scope and did not run afoul of what she was permitted to look for. Based on

all of the collective information, the exclusionary rule should not bar the admission of evidence seized by officers acting in reasonable reliance on the search warrant. The warrant was sought and executed in good faith and as such the Leon exception should be applied to this case.

IV. CONCLUSION

For the preceding reasons, the Court should deny Defendant's Motion to Suppress Evidence.

Dated: February 3, 2023

MAC SCHNEIDER
United States Attorney

By: */s/ Jennifer Klemetsrud Puhl*
JENNIFER KLEMETSRUD PUHL
Assistant United States Attorney
ND Bar ID 05672
655 First Avenue North, Suite 250
Fargo, ND 58102-4932
(701) 297-7400
jennifer.puhl@usdoj.gov
Attorney for United States

By: /s/ Charles Schmitz
CHARLES SCHMITZ
Trial Attorney
Criminal Division
U.S. Department of Justice
(202) 913-4778
Charles.Schmitz2@usdoj.gov